The SAT+CAS Paradigm and the Williamson Conjecture (Extended Abstract)

Curtis Bright
University of Waterloo

Ilias Kotsireas
Wilfrid Laurier University

Vijay Ganesh
University of Waterloo

Abstract

We employ tools from the fields of symbolic computation and satisfiability checking—namely, computer algebra systems and SAT solvers—to study the Williamson conjecture from combinatorial design theory and increase the bounds to which Williamson matrices have been enumerated. In particular, we completely enumerate all Williamson matrices of orders divisible by 2 or 3 up to and including 70. We find one previously unknown set of Williamson matrices of order 63 and construct Williamson matrices in every even order up to and including 70. This extended abstract outlines a preprint currently under submission [4].

1 Introduction

In recent years SAT solvers have been used to solve or make progress on mathematical conjectures which have otherwise resisted solution [10, 11, 13] and in this work we apply a SAT solver to the Williamson conjecture from combinatorial design theory. Our work is similar in spirit to the aforementioned works but we would like to highlight two main differences. Firstly, we employ a programmatic SAT solver as introduced by [9]. A programmatic SAT solver is able to learn conflict clauses *programmatically*, through a piece of code compiled with the SAT solver. This code is specifically tailored to the problem domain and encodes domain-specific knowledge that an off-the-shelf SAT solver would otherwise not be able to exploit. This framework is not limited to any specific domain; any external library or function can be used as long as it is callable by the SAT solver. We show that the clauses that are learned in this fashion can enormously cut down the search space as well as the solver's runtime.

Secondly, similar in style to [17] we incorporate functionality from computer algebra systems to increase the efficiency of the search in what we call the "SAT+CAS" paradigm. This approach of combining computer algebra systems with SAT or SMT solvers was also independently proposed at the conference ISSAC [1]. More recently, it has been argued by the SC^2 project [2] that the fields of satisfiability checking and symbolic computation are complementary and combining the tools of both fields (i.e., SAT solvers and computer algebra systems) in the right way can solve problems more efficiently than could be done by applying the tools of either field in isolation, and our work provides evidence for this view. Specifically, our work uses the MAPLE CAS function `nsoks` [14] and the C library FFTW [8].

Previously [5] we enumerated Williamson matrices of even order up to order 64 and this work extends the enumeration to order 70 and extends the method to enumerate Williamson matrices with orders divisible by 3. In doing so, we find a previously undiscovered set of Williamson matrices of order 63, the first new set of Williamson matrices of odd order discovered since one of order 43 was found over ten years ago [12].

2 The Williamson Conjecture

Williamson introduced the matrices which now bear his name while developing a method of constructing Hadamard matrices—square matrices with ±1 entries and pairwise orthogonal rows [16]. The *Hadamard conjecture* states that Hadamard matrices exist for all orders divisible by 4 and Williamson's construction has been extensively used to construct Hadamard matrices in many different orders. Four matrices A, B, C, $D \in \{\pm 1\}^{n\times n}$ are *Williamson matrices* if they are symmetric, circulant, and $A^2 + B^2 + C^2 + D^2$ is the scalar matrix $4nI$. The *Williamson conjecture* states that Williamson matrices can be used to construct Hadamard matrices in any order divisible by 4; Turyn states it as follows [15]:

> Only a finite number of Hadamard matrices of Williamson type are known so far; it has been conjectured that one such exists of any order $4t$.

Williamson matrices have also found use in digital communication systems and this motivated mathematicians from NASA's Jet Propulsion Laboratory to construct Williamson matrices of order 23 while developing codes allowing the transmission of signals over a long range [3]. These Williamson matrices were consequently used to construct a Hadamard matrix of order $4 \cdot 23 = 92$ [6].

The Williamson conjecture was shown to be false by Đoković [7] who showed that such matrices do not exist in order 35. Later, when an enumeration of Williamson matrices for odd orders up to 59 was completed [12] it was found that Williamson matrices also do not exist for orders 47, 53, and 59 but exist for all other odd orders under 65 since Turyn's construction [15] works in orders 61 and 63. Our work provides for the first time a complete enumeration of Williamson matrices in the orders 63, 66, 68, 69, and 70. In particular, we show that Williamson matrices exist in every even order up to 70.

3 Conclusion

Our work shows the power of the SAT+CAS paradigm (i.e., the technique of applying the tools from the fields of satisfiability checking and symbolic computation) as well as the power and flexibility of the programmatic SAT approach. Our focus was applying the SAT+CAS paradigm to the Williamson conjecture from combinatorial design theory, but we believe the SAT+CAS paradigm shows promise to be applicable to other problems and conjectures. However, the SAT+CAS paradigm is not something that can be effortlessly applied to problems or expected to be effective on all types of problems and our work gives some guidance about the typical kind of problems in which the SAT+CAS paradigm can be expected to work particularly well.

References

[1] Erika Ábrahám. Building bridges between symbolic computation and satisfiability checking. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2015, Bath, United Kingdom, July 6–9, 2015*, pages 1–6, 2015.

[2] Erika Ábrahám, John Abbott, Bernd Becker, Anna M. Bigatti, Martin Brain, Bruno Buchberger, Alessandro Cimatti, James H. Davenport, Matthew England, Pascal Fontaine, Stephen Forrest, Alberto Griggio, Daniel Kroening, Werner M. Seiler, and Thomas Sturm. SC^2: Satisfiability checking meets symbolic computation (project paper). In *Intelligent Computer Mathematics: 9th International Conference, CICM 2016, Bialystok, Poland, July 25–29, 2016, Proceedings*, pages 28–43, Cham, 2016. Springer International Publishing.

[3] Leonard Baumert, S. W. Golomb, and Marshall Hall. Discovery of an Hadamard matrix of order 92. *Bull. Amer. Math. Soc.*, 68(3):237–238, 1962.

[4] Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. Applying computer algebra systems and SAT solvers to the Williamson conjecture. `https://arxiv.org/abs/1804.01172`, 2018.

[5] Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. A SAT+CAS method for enumerating Williamson matrices of even order. In *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence, New Orleans, Louisiana, USA, February 2–7, 2018*, pages 6573–6580, 2018.

[6] Julie Cooper. Hadamard matrix. `https://www.jpl.nasa.gov/blog/2013/8/hadamard-matrix`, 2013.

[7] Dragomir Ž Đoković. Williamson matrices of order $4n$ for $n = 33, 35, 39$. *Discrete mathematics*, 115(1):267–271, 1993.

[8] Matteo Frigo and Steven G Johnson. The design and implementation of FFTW3. *Proceedings of the IEEE*, 93(2):216–231, 2005.

[9] Vijay Ganesh, Charles W. O'Donnell, Mate Soos, Srinivas Devadas, Martin C. Rinard, and Armando Solar-Lezama. Lynx: A programmatic SAT solver for the RNA-folding problem. In *Theory and Applications of Satisfiability Testing - SAT 2012 - 15th International Conference, Trento, Italy, June 17–20, 2012. Proceedings*, pages 143–156, 2012.

[10] Marijn J. H. Heule, Oliver Kullmann, and Victor W. Marek. Solving and verifying the Boolean Pythagorean triples problem via cube-and-conquer. In *Theory and Applications of Satisfiability Testing - SAT 2016 - 19th International Conference, Bordeaux, France, July 5–8, 2016, Proceedings*, pages 228–245, 2016.

[11] Marijn JH Heule. Schur number five. In *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence, New Orleans, Louisiana, USA, February 2–7, 2018*, pages 6598–6606, 2018.

[12] Wolf H Holzmann, Hadi Kharaghani, and Behruz Tayfeh-Rezaie. Williamson matrices up to order 59. *Designs, Codes and Cryptography*, 46(3):343–352, 2008.

[13] Boris Konev and Alexei Lisitsa. A SAT attack on the Erdős discrepancy conjecture. In *Theory and Applications of Satisfiability Testing - SAT 2014 - 17th International Conference, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14–17, 2014. Proceedings*, pages 219–226, 2014.

[14] Joe Riel. `nsoks`: A Maple script for writing n as a sum of k squares. `http://www.swmath.org/software/21060`, 2006.

[15] Richard J Turyn. An infinite class of Williamson matrices. *Journal of Combinatorial Theory, Series A*, 12(3):319–321, 1972.

[16] John Williamson. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J*, 11(1):65–81, 1944.

[17] Edward Zulkoski, Curtis Bright, Albert Heinle, Ilias Kotsireas, Krzysztof Czarnecki, and Vijay Ganesh. Combining SAT solvers with computer algebra systems to verify combinatorial conjectures. *Journal of Automated Reasoning*, 58(3):313–339, Mar 2017.